

## Best Practices in Data Protection Strategies and Due Diligence for Corporations

### Information Strategy

- Develop a “transparency strategy” that determines how closed or open the company needs to be based on the services provided.

### Insider Threat Programs and Awareness

- Institute security training and awareness campaigns; convey threats to company information accessed through portable devices and when traveling abroad.
- Establish an insider threat program that consists of information technology-enabled threat detection, foreign travel and contact notifications, personnel security and evaluation, insider threat awareness and training, and reporting and analysis.
- Conduct background checks that vet users before providing them company information.
- Implement non-disclosure agreements with employees and business partners.
- Establish employee exit procedures; most employees who steal intellectual property commit the theft within one month of resignation.

### Effective Data Management

- Get a handle on company data—not just in databases but also in e-mail messages, on individual computers, and as data objects in web portals; categorize and classify the data, and choose the most appropriate set of controls and markings for each class of data; identify which data should be kept and for how long. Understand that it is impossible to protect everything.
- Establish compartmentalized access programs to protect unique trade secrets and proprietary information; centralize intellectual property data—which will make for better security and facilitate information sharing.
- Restrict distribution of sensitive data; establish a shared data infrastructure to reduce the quantity of data held by the organization and discourage unnecessary printing and reproduction.

### Network Security, Auditing, and Monitoring

- Conduct real-time monitoring/auditing of the networks; maintain thorough records of who is accessing servers, and modifying, copying, deleting, or downloading files.
- Install software tools—content management, data loss prevention, network forensics—on individual computer workstations to protect files.

- Encrypt data on servers and password-protect company information.
- Incorporate multi-factor authentication measures—biometrics, PINs, and passwords combined with knowledge-based questions—to help verify users of information and computer systems.
- Create a formal corporate policy for mobility—develop measures for centrally controlling and monitoring which devices can be attached to corporate networks and systems and what data can be downloaded, uploaded, and stored on them.
- Formalize a social media policy for the company and implement strategies for minimizing data loss from on-line social networking.

### Contingency Planning

- Establish a continuity of operations plan—back up data and systems; create disaster recovery plans; and plan for data breach contingencies.
- Conduct regular penetration testing of company infrastructure as well as of third-party shared service provider systems.
- Establish document creation, retention, and destruction policies.

### Resources for Help

- Contact ONCIX or the FBI for assistance in developing effective data protection strategies. If a data breach is suspected, contact the FBI or other law enforcement/organizations for help in identifying and neutralizing the threat.